REMARKS/ARGUMENTS

The Examiner rejected claims 1-4, 7-30, and 33-40 as obvious (35 U.S.C. §103) over Ananda (U.S. Patent No. 5,495,411) in view of Takahashi (U.S. Patent No. 6,195,432). Applicants traverse for the following reasons.

Independent claims 1, 16, and 27 concern distributing computer software from a first computer system, and require: maintaining keys of all authorized users of software to be distributed; receiving a request for software from a second computer system; generating a message; encrypting the generated message; transmitting the encrypted message to the second computer system; receiving an encrypted response from the second computer system; determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response; decrypting the encrypted response with the determined key if there is one determined key; processing the decrypted response to determine whether the second computer system is authorized to access the software, wherein the second computer system is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response; and permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

Applicants amended claims 1, 16, and 27 to require that the first computer system maintain keys of all authorized users of software to be distributed; determining whether there is one maintained key for the second computer system; the second computer system is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response. These added limitations are disclosed on at least page 6, lines 14-20 and pg. 7, line 14 to pg. 8, line 15 of the Specification.

In rejecting these claims, the Examiner cited col. 11, lines 45-60 and col. 12, lines 15-46 of Ananda as teaching various claim limitations. The cited col. 11 mentions that the password generation module 321E generates a new authorization verification password that is stored as a function of the processor clock time. Note, the cited password generation module 321E is part of the user computer 102 (FIG. 2) because it is part of the header software 284A shown in FIG. 3. Ananda mentions that as shown in FIG. 2, the application software 284B is integrated with header software 284A, which comprises the rental application software 284. (Col. 9, lines 50 to col. 10, line 40. The rental security manager prepares and encrypts a message having information on the user (the user clock time, user ID password, and ID number of the application), which is sent to the multiuser controller 222 at the central facility that enables access to the software.

Nowhere does this cited col. 11 anywhere disclose the claim requirements that the rental manager or other related component, which is in the user computer, maintain keys for authorized users of the software, where the keys are used to decrypt encrypted responses and that the second computer (user computer) is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response. Instead, the cited col. 11 discusses how the user computer generates a message to send to the central facility 180. Because the cited col. 11 concerns operations of the user computer to generate an authorization verification password, nowhere does the cited col. 11 disclose the claim requirements of maintaining keys for authorized users of the software, where the keys are used to decrypt responses to determine whether the second computer providing the response is authorized to use the software.

The cited col. 12 discusses how the multiuser controller 222, part of the database that distributes the software, generates and encrypts a new message, and sends the message to the user as part of an authorization verification process. The rental security manager 321 in the user computer receives the message. The rental security manager 321 is part of the user computer because it is part of the header software 284A shown in FIG. 3. The user computer decrypts the message and has a password validation module 321 that uses a password correlation algorithm to compare the message against stored information regarding the user processor clock time, id, etc.. When the correlation function is successful, authorization verification is complete and the header 320 in the user computer allows application software to execute.

The cited col. 12 discusses how components in the user computer compare a message from the central facility to determine whether the application can continue to execute. Nowhere does the cited col. 12 anywhere disclose the claim requirement of maintaining keys for authorized users of the software, where the keys are used to decrypt encrypted responses and that the second computer is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response. Instead, the cited col. 12 discusses how the user computer can correlate the content of a message with stored information to determine whether the application can start running. The cited col. 12 does not teach maintaining keys to use to verify whether a user requesting access is authorized as claimed. Instead, with the cited col. 12, the authorization is done at the user system, not at the central facility.

The Examiner further cited col. 2, lines 10-25 and col. 5, lines 32-36 of Takahashi as teaching the requirements of using a key for decryption made available by the second computer. (Office Action, pg. 5) The cited col. 2 of Takahashi discusses how when a customer purchases software, the customer generates a shared key to use to communicate with a store and encrypts the shared key and sends the shared key to the store. The store decrypts the shared key and stores it. The customer then uses the shared key to encrypt information being sent to the store.

The cited col. 5 of Takahashi discusses how the customer software distribution system registers user charge information and a shared key shared between the provider and the user. The server uses the shared key to encrypt software to download to the customer. (Takahashi, col. 5, lines 40-47).

Nowhere do the cited cols. 2 and 5 disclose the claim requirements that the system providing access to the software maintain keys for authorized users of the software, where the keys are used to decrypt encrypted responses and that the second computer is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response. The cited cols. 2 and 5 discuss how the server maintains a shared key that is used to encrypt software to download to the customer. However, the cited cols. 2 and 5 nowhere teach or suggest the claim requirements that a determination is made whether there is a key to decrypt a response from the user and then using the presence or absence of that key to determine whether the requestor may access the software. Instead, with the cited Takahashi, the shared key is used to send the software to the user, not used by the server to decrypt an encrypted response and denying access to the software if there is not one maintained key capable of decrypting the encrypted response.

For all the above reasons, the amended claims 1, 16, and 27 are patentable over the cited combination, because the cited references, alone or in combination, do not teach or suggest all the claim requirements.

Claims 2-4, 8-11, 17-19, 21-24, 28-30, and 34-40 are patentable over the cited art because they depend, directly or indirectly, from one of claims 1, 16, and 27. Moreover, certain of these claims provide additional grounds of patentability over the cited art for the reasons discussed below.

Amended claims 4, 19, and 30 depend from claims 1, 16, and 27, respectively, and further require that generating the message further comprises generating a random component to include within the message, and that determining whether the second computer system is authorized to access the software further comprises determining whether the decrypted response includes the generated message transmitted to the second computer system, wherein the second computer system is authorized to access the software if the decrypted response includes the generated message.

Nowhere does the cited Ananda anywhere disclose that the first computer system or central facility, determine whether the user is authorized to access the software by determining whether the decrypted response includes a generated message the first computer system, or central facility, sent to the user (second computer system.)

Instead, with the cited Ananda, components in the user computer determine whether access may continue. The cited Ananda does not have the central facility determine whether the user (second computer system) may access the software by checking whether the encrypted response has a generated message the first computer system (central facility) previously sent as claimed.

Accordingly, amended claims 4, 19, and 30 provide additional grounds of patentability over the cited art.

Claims 8, 21, and 34 depend from claims 1, 16, and 27, respectively, and further require that processing the encrypted response further comprises determining whether a message included in the encrypted response matches the generated message, wherein the second computer is authorized to access the software if the message included in the encrypted response matches the generated message.

The cited Ananda does not disclose that the first computer system (or central facility in Ananda) determines whether the message in the encrypted response from the second computer system matches the generated message the first computer system initially sent to the second computer system. Instead, the cited Ananda has the user computer system compare stored information with a message from the central facility, likened to the first computer system, to determine whether access is permitted. Nowhere does the cited Ananda anywhere disclose that the central facility, likened to the first computer system, compare a message in an encrypted response from the user computer, likened to the second computer system, to determine whether it matches the generated message the central facility (first computer system) previously sent to the user computer (second computer system). Thus, the cited operations of Ananda are different from the claimed operations.

Accordingly, claims 8, 21, and 34 provide additional grounds of patentability over the cited art.

Applicants amended claims 9, 11, 22, 24, 35, and 37 to specify that the maintained keys comprise public keys. These claims are patentable over the cited art because the combination of the dependent claim requirement with the base claims provide further grounds of distinction over the cited art.

Amended independent claims 12 and 25 concern accessing computer software from a first computer system with a second computer system and require that the second computer system perform: providing a key to the first computer system capable of decrypting an encrypted response from the from the second computer system; transmitting a request for the software to the first computer system; receiving an encrypted message from the first computer system; processing the encrypted message to generate a response message; encrypting the response message, wherein the encrypted response message is capable of being decrypted by the provided key at the first computer system; transmitting the encrypted response message to the first computer system; and receiving access to the requested software in response to the encrypted response message.

Applicants amended claims 12 and 15 to recite that the code comprises a key.

The Examiner cited the same sections of Ananda against claims 12 and 25 that were cited against independent claims 1, 16, and 27.

The cited Ananda discusses how a user computer generates an authorization verification password and sends an encrypted message with various information to the central facility. A multi-user controller 22 at the central facility generates a message to send back to the user computer. The user computer header software then verifies the received message from the central facility with the stored authorization verification password.

Nowhere does the cited Ananda anywhere teach or suggest the claim requirement of the second computer (user computer) providing a key to the first computer, and then transmitting a response to the first computer that can be decrypted by the sent key, and then receiving access to the requested software in response to the encrypted response message.

The cited Takahashi discusses how the customer software distribution system registers user charge information and a shared key shared between the provider and the user. The server uses the shared key to encrypt software to download to the customer.

Further, the cited Takahashi discusses how the customer requests the software and that the server downloads the software encrypted using the key. However, nowhere does the cited Takahashi anywhere teach or suggest the claim requirement that the customer encrypt the response message that can be decrypted using the key previously provided.

Accordingly, claims 12 and 25 are patentable over the cited Ananda because Ananda does not disclose the claim requirements.

Claims 13-15 and 26 are patentable over the cited art because they depend from claims 12 and 25, respectively, which are patentable over the cited art for the reasons discussed above.

Claims 38-40 are patentable over the cited art because they depend, directly or indirectly, from claim 26, which is patentable over the cited art for the reasons discussed above.

The Examiner rejected claims 5, 6, 31, and 32 as obvious (33 U.S.C. 103) over Ananda in view of Komura (U.S. Patent No. 5,994,307). Applicants traverse this rejection on the grounds that these claims depend from claims 1, 16, and 27, which are patentable over the cited art for the reasons discussed above. Moreover, these claims provide additional grounds of patentability over the cited art for the reasons discussed below.

First off, claims 5, 6, 31, and 32 are patentable over the cited art because they depend from claims 1, 16, and 27, which are patentable over the cited art for the reasons discussed above. Further, these claims provide additional grounds of distinction over the cited art for the following reasons.

Claims 5 and 31 depend from claims 1 and 27, respectively, and further require that the random component is comprised of a time stamp. The Examiner cited Komura as teaching the time stamp claim requirement. (Office Action, pg. 7) Applicants traverse.

Although the cited Komura does discuss a timestamp and Ananda mentions that a clock time is used to calculate a pseudo number password, nowhere does the cited Ananda, Takahashi or Komura, alone or in combination, anywhere teach or suggest that a message generated and encrypted and sent to a second computer system, which is then included in an encrypted response by the second computer system to the first computer system, comprises a timestamp.

Accordingly, claims 5 and 31 provide additional grounds of patentability over the cited art.

Claims 6 and 32 depend from claims 5 and 31 and further require that the time stamp is inserted at an offset into the message. These claims are patentable over the cited combination because they depend from claims 5 and 31, which are patentable over the cited art for the reasons discussed above, and because they provide further requirements on the timestamp, which is not disclosed in the cited Ananda.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1-40 are patentable over the art of record. Applicants submit herewith the fee for a one-month extension of time. Nonetheless, should any additional fees be required, please charge Deposit Account No. 09-0466.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: December 9, 2004

By:____________________
David W. Victor
Registration No. 39,867

Please direct all correspondences to:

David Victor
Konrad Raynes & Victor, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977
Fax: 310-556-7984